|  |  |
| --- | --- |
| **Document Name** | **Incident Management Policy** |
| **Version** | **0.2** |
| **Last Updated By** | **Anjaly T A** |
| **Approved By** | **Inderjit Singh Bedi** |
| **Released on** | **23-08-2022** |

Contents

[1. Overview 3](#_Toc61454917)

[2. Purpose 3](#_Toc61454918)

[3. Scope 3](#_Toc61454919)

[4. Contingency Plans 3](#_Toc61454920)

[5. Policy Compliance 3](#_Toc61454921)

[5.2 Exceptions 4](#_Toc61454922)

[5.3 Non-Compliance 4](#_Toc61454923)

# Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives the organization a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

# Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by Xtracap that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

# Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is to highlight the contingencies that may arise in the business and the basic manner to tackle these issues.

# Contingency Plans

The following are the contingency plans:

* + 1. Computer Emergency Response Plan:For any computer emergency response plans, employees must contact the IT Infra Lead – Inderjit Singh Bedi.   
       It is advisable that all data in machines of all individuals must be kept on the Cloud Service being used by the company and on the local memory. Any employee that faces any issue with the computer must contact the aforementioned lead immediately
    2. Criticality of Service List:A list of all critical services can be found in the Cloud in the Shared Folder which is accessible to all employees.
    3. Data Backup and Restoration Plan:Data on Production is backed up on a real-time basis on the DR server. Backups of all servers are also automatically downloaded daily to our premises. Weekly backups are maintained offshore with the business. Based on the need of the incident, data recovery will
    4. Equipment Replacement Plan:For any equipment replacement place a complaint with the IT Infra Lead. Based on the severity and the need of the equipment, the turn around time to receive the replacement will vary.

# Procedure

In case of any incident, the Internal IT team consisting of developers and IT Infra Lead will take the appropriate actions to solve the incident and publish a root-cause analysis along with the fixes. The severity of the incident will decide the priority and manpower needed to fix it.

# Policy Compliance

6.1 Compliance Measurement

The IT Infra team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

# Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

# Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.